Software Testing and Verification

Problem Set 6: Predicate Transforms

1. Consider the assertion of *weak* correctness: {t=5 Λ z<0} s {y=z+1 Λ t=z}. Which of the following observations/facts would allow one to deduce that the assertion is FALSE and which would not? Consider the observations individually and briefly justify your answer for each.

   a. The wp(s, y=z) is z>-5.
   b. The wlp(s, y=z) is z>-5.
   c. (t=5 Λ z<0) ≠> wlp(s, y=z+1 **V** t=z) (Note the logical **OR**.)
   d. ["sp(s, t=5 Λ z>-5) is undefined"] Λ [sp(s, t=5 Λ z≤-5) => (y=z+1 Λ t=z)]

2. Consider the program:

```
temp := x
x := y
y := temp
if temp>z then
   y := z
   z := temp
   if x>y then
      temp := x
      x := y
      y := temp
   end_if
end_if
```

   Under what circumstances will the program result in {x≤y<z}? (Hint: determine the wp of the program w.r.t. the desired result.)

3. We have learned that (P => wp(s,Q)) implies ({P} s {Q}). However, ({P} s {Q}) does NOT imply (P => wp(s,Q)). Why?

4. a. Use the wlp rule for while-do statements given in Lecture Notes 20 to find the weakest liberal pre-condition of the following program with respect to the post-condition Z=XY.

```
while J<>Y do
   Z := Z+X;
   J := J+1
end_while
```

b. Consider the invariant, I: Z=XJ, used with the while-loop ROI to prove the assertion given on slide 11 of Lecture Notes 18. How does it compare in "strength" to the weakest liberal pre-condition from part (a) above? (In particular, is one STRONGER than the other?) Briefly explain your answer.

5. Prove "finalization" of the weakest liberal pre-condition of a while statement. That is, prove the tautology:

$$(wlp(\text{while } b \text{ do } s, Q) \wedge \sim b) \Rightarrow Q.$$

6. a. Identify H_1, H_2, H_3, and H_k such that

$$wp(\text{Repeat } s \text{ Until } c, Q) = H_1 \vee H_2 \vee H_3 \vee \ldots \vee H_k \vee \ldots$$

where H_i represents the necessary and sufficient condition that "Repeat s Until c" terminates in state Q after i executions of s. For i>1, H_i should be expressed as a function of H_{i-1}.

b. Use your formulations to determine the weakest pre-condition of:

```
Repeat
   x := x+1;
   y := y-1
Until y=0
```

with respect to the post-condition: x=17. (Show the values of H_1, H_2, H_3, and H_k, and then express the result in closed form.)